REMARKS

Claims 1-3, 10-12, 22-33 and 37-48 are pending in the present application. Claims 1-3, and 10-12 were amended in this response. Claims 19-21, 34 and 36 were cancelled, without prejudice. No new matter has been introduced as a result of the amendments.

Claims 1-3, 10, 19-33, 37, 40, 43 and 46 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Kilner* (US Patent 5,649,089) in view of *Frezza et al.* (US Patent No. 4,982,430) and *McNamara* (US Patent 4,533,948).

Claims 11, 12, 34, 36, 38, 39, 41, 42, 44, 45, 47 and 48 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Kilner* (US Patent 5,649,089) in view of *Frezza et al.* (US Patent No. 4,982,430) and *McNamara* (US Patent 4,533,948) and further in view of *Mattison* (US Patent 5,778,070). Applicants respectfully traverse these rejections. Favorable reconsideration is earnestly requested.

Specifically, the cited art, alone or in combination, does not teach forming segment checksums in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function as recited in claim 1, and similarly recited in claims 2-3 and 10-12. Under the recited configuration, a method for checking the integrity of digital data grouped into data segments is disclosed where flow control for the individual data segments is no longer required. According to the claims, commutative checksums are formed by a commutative operation on segment checksums formed from a hashing value and a cryptographic one-way function. This has an advantageous effect of detecting error to a greater degree of precision (e.g., one bit errors under all conditions using hash values).

In contrast, *Kilne*r discloses a configuration where a cyclic redundancy checksum (CRC) code is used to protect data fields against modification (col. 3, lines 36-50), but is silent regarding the use of a hashing value or a cryptographic one-way function. In fact, Kilner teaches away from the use of such functions (see col. 1, lines 41-55). Furthermore, *Frezza* does not solve the deficiencies of *Kilner* discussed above. *Frezza* discloses a communication system where users are allowed to securely download data from a remote site (col. 1, line 55-col. 2, line 9). During a download process, booter data is downloaded to a user terminal from a booter 14 to establish a subscriber identity (col. 4, lines 18-46). Subsequently, a checksum operation is performed on the booter data to validate the user, and an encrypted communication link is established with the terminal to the network control center (NCC) by transmitting the encrypted checksum (col. 5, line 39 - col. 6, line 19). Thus, Frezza also fails to teach or suggest cryptographically protecting a commutative checksum that is formed by a commutative operation on the first segment checksums. Furthermore, the CRC check performed in Kilner would not be properly combined with the teaching in Frezza, as the checksum operation on the booter data in Frezza would not be compatible with the CRC operation of Kilner (see MPEP 2143.01)

In light of the above, Applicants respectfully submit that independent claims 1-3 and 10-12 of the present application, as well as claims 19-34 and 36-48 which respectively depend therefrom, are both novel and non-obvious over the art of record. Accordingly, Applicants respectfully request that a timely Notice of Allowance be issued in this case. If any additional fees are due in connection with this application as a whole, the Examiner is authorized to deduct said fees from Deposit Account No.: 02-1818. If such a deduction is made, please indicate the attorney docket number (0112740-466) on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY ____________________
Peter Zura
Reg. No. 48,196
Customer No.: 29177
Phone: (312) 807-4208

Dated: August 1, 2006